

The Strength of Network Based Authentication

ID Analytics for Authentication is a cost-effective, network based authentication solution that uses identity intelligence to authenticate individuals at critical points of interaction including account origination, identity proofing, high-risk transactions, and profile changes. This proprietary and effective approach has been proven to eliminate customer friction, lower abandonment rates, and reduce operational costs.

id:analytics™

Based on an evaluation of millions of desirable and suspicious behaviors and relationships, ID Analytics for Authentication gains the insight required to dynamically generate authenticating questions that are unique to an individual. Network based authentication sessions rely on a real-time, high-resolution view of each individual's particular identity characteristics including connectedness to other individuals and their unique identity characteristics. This ability to deliver on-demand identity intelligence is why the top U.S. communication and financial service companies, as well as major retailers, government agencies and healthcare insurers, all trust ID Analytics to drive new revenue opportunities, eliminate financial losses, and facilitate compliance with federal regulations.

How It Works

By understanding the complex information patterns and linkages that make up an individual identity, ID Analytics for Authentication assesses the risk of an individual identity and determines whether further authentication is necessary. ID Analytics for Authentication uses ID Score®-Risk to deliver the complete, cross-industry view of identity risk at any point in the customer lifecycle.

THE BENEFITS OF ID ANALYTICS FOR AUTHENTICATION

- **Gain Cost-Efficiencies**
Achieve cost savings of up to 50% compared to knowledge based authentication solutions that rely on public records data and credit history information.
- **Detect Synthetic and Stolen Identities**
The ID Network contains detailed information on more than 2 million reported frauds and is continually updated with millions of new identity elements daily.
- **Leverage Identity Intelligence**
Data within the ID Network has been proven effective within emerging market segments such as young professionals which often lack public-record details and credit histories required to generate knowledge-based authentication questions.
- **Seamless Integration**
As a hosted solution, ID Analytics for Authentication supplements existing decisioning processes via a standardized API or web-based interface.

$$u(x) = \beta_0 + \sum_{i=1}^n \beta_i x_i$$

If the risk of identity fraud is high, Certain ID™ is then used to generate and deliver strong authentication questions. This ensures that legitimate customers are not inconvenienced and their transactions can be processed efficiently.

ID Score-Risk

As a network based authentication solution, ID Analytics for Authentication does not rely on public records data that is easily accessible by identity thieves. The result is a strong, yet cost-effective consumer authentication solution based on identity intelligence and the industry's most accurate identity risk analytics. ID Score-Risk leverages data within the proprietary ID Network® – the nation's only real-time, cross-industry compilation of identity information – to provide clarity to the complex information patterns that make up an individual identity while detecting synthetic and stolen identities.

By extending the ID Network to include personal identity information as well as online identity elements such as Internet protocol (IP) addresses, device fingerprints, email addresses, and IP geo-location data, ID Analytics for Authentication addresses the specific challenges of customer-not-present interactions. In fact, the same online identity elements that render third-party data verification tools ineffective actually increase the effectiveness of ID Score-Risk. ID Score-Risk delivers the identity intelligence required to automatically govern the sophistication of a network based authentication session. For low-risk identities, this may even include bypassing authentication questions altogether in order to preserve a positive customer experience and reduce abandonment of legitimate interactions.

Certain ID

Certain ID generates and delivers strong authentication questions that are top of mind for legitimate individuals. These questions are based on data from the ID Network, not public-records data. In addition to cross-industry data elements, the ID Network contains detailed information on two million reported frauds. The unique identity information within the ID Network ensures that Certain ID creates questions that are very difficult for someone perpetuating identity fraud to answer correctly. By avoiding dependence on publicly available information, ID Analytics for Authentication delivers a cost-effective solution while strengthening consumer authentication processes.

Certain ID may be customized for your specific business needs. This flexibility allows companies to modify the number of questions asked, the types of questions asked, and the number of correct answers required for authentication. In fact, the number of correct answers required can be dynamically escalated for high risk identities.

Leverage the Strength of Network Based Authentication

Turn to ID Analytics for Authentication to eliminate customer friction, lower abandonment rates, and reduce operational costs. Contact us at marketinginfo@idanalytics.com, 858-312-6200, or 866-248-7344 to discover how network based authentication can benefit your business. Or, visit www.idanalytics.com for more information about our identity intelligence solutions.

“ The best way to protect consumers from identity fraud is to focus resources precisely where the potential harm from this fraud exists: where new accounts are being opened, credit is being granted, and identification is being issued. ”

- American Banker

STRENGTHENING CONSUMER AUTHENTICATION PROCESSES

ID Analytics for Authentication is easy to integrate within existing call center and online environments. The choice of a packaged client browser or standard Application Programming Interface delivers the flexibility to deploy across a variety of critical consumer interactions including:

- **Account Origination**
Creditors report that the attempted fraud rate for online applications can be up to 10 times greater than paper based forms. Authentication questions provide an additional layer of fraud protection that benefits businesses and consumers.
- **Identity Proofing**
These critical processes support the issuance of re-usable credentials such as tokens, passwords, or device registrations used to perform ongoing account management and self-service. While credentials are authenticated in every transaction, the identity associated with the credential is authenticated once – during the initial identity proofing process.
- **High-Risk Transactions**
Automated, online authentication questions work within existing fraud detection processes to reduce manual review costs and eliminate transaction delays.
- **Profile Changes**
Requests for password resets, address changes, or suspicious account requests received online or via call centers require on-demand identity intelligence.